

Maximally Non-Local and Monogamous Quantum Correlations

Jonathan Barrett,^{1,*} Adrian Kent,^{2,†} and Stefano Pironio^{3,‡}

¹*Perimeter Institute for Theoretical Physics, 31 Caroline Street N, Waterloo, Ontario N2L 2Y5, Canada*

²*Centre for Quantum Computation, DAMTP, Centre for Mathematical Sciences,*

University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, U.K.

³*ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*

Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125, U.S.A.

(Dated: May 19, 2006)

We introduce a version of the chained Bell inequality for an arbitrary number of measurement outcomes, and use it to give a simple proof that the maximally entangled state of two d dimensional quantum systems has no local component. That is, if we write its quantum correlations as a mixture of local correlations and general (not necessarily quantum) correlations, the coefficient of the local correlations must be zero. This suggests an experimental programme to obtain as good an upper bound as possible on the fraction of local states, and provides a lower bound on the amount of classical communication needed to simulate a maximally entangled state in $d \times d$ dimensions. We also prove that the quantum correlations violating the inequality are monogamous among non-signalling correlations, and hence can be used for quantum key distribution secure against post-quantum (but non-signalling) eavesdroppers.

Quantum theory predicts that measurements on separated entangled systems will produce outcome correlations that, in Bell's terminology [1], are not *locally causal* or, in what has become standard terminology, are *non-local*. In particular, if a Bell inequality is violated then one cannot consistently assume that the outcomes of measurements on each system are predetermined and independent of the measurements carried out on the other system(s). Violation of Bell inequalities has been confirmed in numerous experiments [2].

Violation of Bell inequalities not only tells us something fundamental about Nature, but also has practical applications. For example, the nonlocality of quantum correlations allows communication complexity problems to be solved using an amount of communication that is smaller than is possible classically [3]. Barrett-Hardy-Kent (BHK) recently showed that testing particular nonlocal quantum correlations allows two parties to distribute a secret key securely, in such a way that the security is guaranteed by the no-signalling principle alone [4] (i.e. without relying on the validity of quantum theory).

In this paper, we extend the chained Bell inequality to an inequality with an arbitrary number of measurement outcomes, which can thus be applied to states in arbitrary dimensions. In the limit of a large number of measurement settings, quantum mechanics predicts correlations for a maximally entangled bipartite state that resemble those of the tripartite Greenberger-Horne-Zeilinger (GHZ) state in that, with probability tending to one, the predictions of any local hidden variable model contradict those of quantum mechanics for at least one pair of measurements. We use this to give a constructive proof of a result originally due to Elitzur, Popescu and Rohrlich (EPR) [5]: if the quantum correlations of a maximally entangled state of two qubits are written as

a convex combination of local and nonlocal correlations, then the local fraction must be zero. Our proof extends EPR's result to maximally entangled states in any dimension and also removes the need for a technical assumption required for EPR's original proof [6]. Moreover, because our proof is constructive, it motivates an experimental programme to establish the best possible upper bound on the fraction of local states in a maximally entangled state. More generally, our proof method works, and motivates experimental tests, for any example of GHZ-type correlations.

Next, we give a rigorous proof of the *monogamy* of the correlations obtained from a $d \times d$ -dimensional maximally entangled state. Here, monogamy means that a third party cannot get any information about the measurement outcomes, so long as a no-signalling condition holds, even if quantum theory is incorrect. This property has a particular significance in the context of secret key distribution, and our results here generalise those of BHK [4], which proved monogamy in the 2×2 -dimensional case in order to demonstrate the security of BHK's scheme against general non-signalling eavesdroppers.

Finally, as a corollary, we derive a lower bound on the classical communication needed to simulate measurements on a maximally entangled state in $d \times d$ dimensions.

Some chained Bell inequalities. Consider a standard Bell-type experiment: two parties, Alice and Bob, share a joint system in an entangled quantum state, and perform measurements on their local subsystems. Each party may choose one out of N different measurements, and each measurement A_k of Alice and B_l of Bob ($k, l = 1, \dots, N$) may have d possible outcomes: $A_k, B_l = 0, \dots, d-1$. Quantum theory predicts the joint probabilities $P^{QM}(A_k = a, B_l = b)$ that Alice's and Bob's measurements, A_k and B_l , have respective outcomes a and b . The correlations predicted by quantum theory are *local*

if and only if they can be written in the form

$$P^{QM}(A_k = a, B_l = b) = \sum_{\lambda} q_{\lambda} P_{\lambda}(A_k = a) \times P_{\lambda}(B_l = b),$$

with $0 \leq q_{\lambda} \leq 1$ and $\sum_{\lambda} q_{\lambda} = 1$. Without loss of generality, we can assume that the terms $P_{\lambda}(A_k = a)$ and $P_{\lambda}(B_l = b)$ are deterministic, that is, that they only take the values 0 or 1 [7]. The correlations are thus local if and only if they can be reproduced by a mixture of hidden states assigning definite values to each measurement. Violation of a Bell inequality implies that the correlations cannot be written in this form.

In general one can write the correlations as

$$P^{QM}(A_k = a, B_l = b) = p P^L(A_k = a, B_l = b) + (1 - p) P^{NL}(A_k = a, B_l = b), \quad (1)$$

where $P^L(A_k = a, B_l = b)$ and $P^{NL}(A_k = a, B_l = b)$ represent local and non-local joint distributions, respectively, and p and $(1 - p)$ their corresponding weights in the mixture, with $0 \leq p \leq 1$. Suppose now that we have a set of quantum correlations which satisfy some relation with certainty, and we can show that any local model must fail to satisfy the relation at least some of the time. It follows that the correlations cannot be written in the form of Eq. (1) except with $p = 0$. (Note that this is true even if the term $P^{NL}(A_k = a, B_l = b)$ is allowed to describe signalling correlations.) A particularly well-known example of such correlations was that produced by GHZ [8] and simplified by Mermin [9]; hence we refer to correlations with these properties as GHZ-type correlations. Bipartite examples have been given by Heywood-Redhead [10] and Cabello [11]. A set of quantum correlations is of GHZ-type if and only if it has an associated Bell inequality which is violated right up to the algebraic limit of the expression.

We now derive a Bell inequality and show that in the limit of a large number of measurement settings, the quantum correlations from a maximally entangled state violate the inequality up to the algebraic limit. Thus the quantum correlations tend to GHZ-type as the number of measurement settings becomes large. Hence, we show, maximally entangled states in any dimension have zero local component.

Consider first the case where Alice and Bob each have a choice between two different measurements ($N = 2$). Local correlations satisfy the following inequality [12],

$$I_2 = \langle [A_1 - B_1] \rangle + \langle [B_1 - A_2] \rangle + \langle [A_2 - B_2] \rangle + \langle [B_2 - A_1 - 1] \rangle \geq d - 1, \quad (2)$$

where $\langle X \rangle = \sum_{i=1}^{d-1} i P(X = i)$ is the average value of the random variable $X \in \{0, \dots, d-1\}$ and $[X]$ denotes X modulo d . This follows from the identity

$$[A_1 - B_1 + B_1 - A_2 + A_2 - B_2 + B_2 - A_1 - 1] = d - 1,$$

and the relation $[X] + [Y] \geq [X + Y]$. When $d = 2$, it corresponds to the CHSH inequality [13].

We can extend the above inequality to an arbitrary number N of measurement choices:

$$I_N = \langle [A_1 - B_1] \rangle + \langle [B_1 - A_2] \rangle + \langle [A_2 - B_2] \rangle + \dots + \langle [A_N - B_N] \rangle + \langle [B_N - A_1 - 1] \rangle \geq d - 1. \quad (3)$$

This extended inequality can be viewed as a chained version of inequality (2), and follows by a similar argument. It is equivalent, when $d = 2$, to the chained inequality introduced by Pearle [14] and Braunstein and Caves [15]. The relation between the Pearle-Braunstein-Caves inequality and GHZ-type correlations was first pointed out by Hardy [16].

We now show that if Alice and Bob share the maximally entangled state

$$|\psi_d\rangle = 1/\sqrt{d} \sum_{q=0}^{d-1} |q\rangle_A |q\rangle_B, \quad (4)$$

there exist measurement settings such that for large N , $I_N(QM)$ tends to zero. The maximally entangled state $|\psi_d\rangle$ has the property that if Alice measures an observable with eigenvectors $|r\rangle$ ($r = 0, \dots, d-1$) and Bob measures the observable with complex conjugate eigenvectors $|r\rangle^*$, they get perfectly correlated outcomes. We define the eigenvectors characterizing Alice's measurement A_k as

$$|r\rangle_{A_k} = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \exp\left[\frac{2\pi i}{d} q(r - \alpha_k)\right] |q\rangle_A, \quad (5)$$

and those characterizing Bob's measurement B_l as

$$|r\rangle_{B_l} = \frac{1}{\sqrt{d}} \sum_{q=0}^{d-1} \exp\left[-\frac{2\pi i}{d} q(r - \beta_l)\right] |q\rangle_B, \quad (6)$$

where $\alpha_k = (k - 1/2)/N$ and $\beta_l = l/N$.

A straightforward calculation shows that each term in (3) is equal to $\gamma/N^2 + O(1/N^3)$, where $\gamma = \pi^2/(4d^2) \sum_{j=1}^{d-1} j/\sin^2(\pi j/d)$. As there are $2N$ such terms in the inequality (3), it follows that

$$I_N(QM) = 2\gamma/N + O(1/N^2), \quad (7)$$

which can be made arbitrarily small for sufficiently large N .

For any particular finite value of N , the quantity $I_N(QM)$ implies an upper bound on the fraction of local states in any model that reproduces the correlations, i.e., an upper bound on the p of Eq. (1). This is because although the term $P^{NL}(A_k = a, B_l = b)$ can violate the Bell inequality (3), it must satisfy $I_N(NL) \geq 0$, since each term in (3) is a positive quantity. Thus we

can write $I_N(QM) = p I_N(L) + (1-p) I_N(NL)$, and, since $I_N(L) \geq d-1$ and $I_N(NL) \geq 0$, $I_N(QM) \geq p(d-1)$, or

$$p \leq \frac{I_N(QM)}{d-1}. \quad (8)$$

Of course, in a real experiment, the state prepared will not be precisely (4), the measurements will not be precisely defined by projections onto the vectors (5) and (6), and so on, and thus the experimentally determined value, $I_N(EXP)$, will generally be greater than $I_N(QM)$. Nonetheless, given a value for $I_N(EXP)$, we can obtain a bound of the form

$$p \leq \frac{I_N(EXP)}{d-1}. \quad (9)$$

Hence we propose an experimental challenge: to obtain the lowest possible bound on p (for any d and N) for bipartite maximally entangled states.

Our proof extends to any example of GHZ-type correlations; thus another natural challenge is to obtain the lowest possible bound on p for any set of quantum correlations on any bipartite or multipartite entangled state.

Indeterminacy of the measurement outcomes and Monogamy. The correlations that we just introduced have a particular significance in the context of key distribution. BHK showed [4] how non-local correlations can be used as the basis of a key distribution scheme that is secure against non-signalling eavesdroppers. Non-local correlations can also be used to give at least partial security against non-signalling eavesdroppers in more practical QKD schemes [17, 18]. In these discussions, it is not assumed that such eavesdroppers are constrained by the laws of quantum mechanics, but it is assumed that they can only prepare systems in states whose correlations are *non-signalling*, in the following sense. Suppose that Alice and Bob share a bipartite system characterized by correlations $P(A_k = a, B_l = b)$. The correlations are non-signalling if they satisfy

$$\sum_a P(A_k = a, B_l = b) = \sum_{a'} P(A_{k'} = a', B_l = b), \quad (10)$$

for all k, k', l, b , and a similar set of conditions obtained by summing over Bob's input. These no-signalling conditions ensure that the marginal distributions $P(A_k = a)$ and $P(B_l = b)$ are well defined quantities. The definition of no-signalling can be extended to more than two parties, by requiring a condition similar to (10) for every possible grouping of the parties into two subsets.

In the protocols of Refs. [4] and [17, 18], maximally entangled states are prepared by a source, which is situated between Alice and Bob and assumed to be under control of the eavesdropper Eve. On each pair of particles, Alice and Bob perform measurements A_k and B_l , chosen independently and randomly, and use the corresponding measurement outcomes to establish a shared secret key.

If the correlations used to distribute the key admit a model with fractions p and $1-p$ of local and non-signalling non-local states respectively, then for a fraction p of pairs, Eve could prepare a deterministic local state that would give her complete information about Alice's and Bob's measurement outcomes. This strategy is clearly not significantly useful to Eve if the quantum correlations imply $p \approx 0$, which is the case in BHK's protocol [4], as noted above.

However, a zero fraction of local states does not necessarily imply that Eve's information is zero, as it does not exclude the possibility that she could prepare a non-local state that has definite values for a non-empty proper subset of the measurement inputs. For instance, in the case of Cabello's example [11], there is a model reproducing the quantum correlations with the following properties: i) every hidden state is non-signalling, ii) for every hidden state, at least one measurement has a predetermined outcome, iii) each measurement has a predetermined outcome for at least some finite fraction of the hidden states. A non-signalling Eve exploiting this model could obtain some knowledge of Alice's and Bob's measurement outcomes. Similar remarks apply to the GHZ and Mermin examples.

The correlations defined by (4), (5) and (6), however, are stronger in the sense that any non-signalling model that reproduces the correlations has the following property: for every hidden state, the outcomes of any measurement are completely undetermined and occur all with the same probability $1/d$. This property is implied by the following theorem.

Theorem. *Any no-signalling distribution for which $I_N \leq I_N^*$ satisfies*

$$P(A_k = a) \leq \frac{1}{d} + \frac{d}{4} I_N^* \quad \text{and} \quad P(B_l = b) \leq \frac{1}{d} + \frac{d}{4} I_N^*$$

for all measurements A_k and B_l and for all outcomes a and b .

In the limit $I_N^* \rightarrow 0$, Eve cannot therefore gain any knowledge about Alice and Bob's measurement outcomes. In other words, any tripartite distribution describing the joint systems of Alice, Bob and Eve is of the form $P(A_k = a, B_l = b) \times P(E_m = e)$. We say that Alice's and Bob's correlations are *monogamous*, in obvious analogy with the familiar monogamy of entanglement.

Proof of the Theorem. Suppose that $P(A_k = a) > 1/d + d/4 I_N^*$ for some measurement A_k and outcome a . We will then show that $I_N > I_N^*$. (The same argument applies if we suppose that $P(B_l = b) > 1/d + d/4 I_N^*$ for some measurement B_l and outcome b .)

Defining $A_{N+1} = A_1 + 1$ (modulo d), we can write

$$\begin{aligned} I_N &= \sum_{j=1}^N (\langle [A_j - B_j] \rangle + \langle [B_j - A_{j+1}] \rangle) \\ &\geq 2N - \sum_{j=1}^N (P(A_j = B_j) + P(A_{j+1} = B_j)), \end{aligned} \quad (11)$$

since $\langle [X] \rangle = \sum_{i=1}^{d-1} i P([X] = i) \geq 1 - P([X] = 0)$. Now

$$\begin{aligned} P(A_i = B_j) &= \sum_{r=0}^{d-1} P(A_i = r, B_j = r) \\ &\leq \min(P(A_i = q), P(B_j = q)) \\ &\quad + \min(1 - P(A_i = q), 1 - P(B_j = q)) \\ &= 1 - |P(A_i = q) - P(B_j = q)|, \end{aligned}$$

for any $q \in \{0, \dots, d-1\}$. Using this expression in the above inequality for I_N and defining N arbitrary different values q_j , we get

$$\begin{aligned} I_N &\geq \sum_{j=1}^N (|P(A_j = q_j) - P(B_j = q_j)| \\ &\quad + |P(A_{j+1} = q_j) - P(B_j = q_j)|) \\ &\geq \sum_{j=1}^N |P(A_j = q_j) - P(A_{j+1} = q_j)|, \end{aligned} \quad (12)$$

where the second line follows from the triangle inequality. The hypothesis $P(A_k = a) > 1/d + d/4 I_N^*$ implies that

$$|P(A_k = a') - P(A_k = a' + 1)| > I_N^*$$

for some a' . If we define the values q_j used in (12) by $q_1 = \dots = q_{k-1} = a'$ and $q_k = \dots = q_N = a' + 1$ (modulo d), we obtain the inequality

$$\begin{aligned} I_N &\geq |P(A_1 = a') - P(A_k = a')| \\ &\quad + |P(A_k = a' + 1) - P(A_{N+1} = a' + 1)| \\ &= |P(A_k = a') - P(A_k = a' + 1)| \\ &> I_N^*, \end{aligned} \quad (13)$$

since $A_{N+1} = A_1 + 1$ (modulo d), by definition. \square

Classical simulation of the correlations. Finally, we note that the bound (8) can be interpreted, in the spirit of [19], as a bound on the average communication necessary to simulate classically non-local correlations. The fact that every hidden state must be non-local in any model that reproduces measurements on a maximally entangled state implies that in any run of a communication-assisted classical protocol some communication must be exchanged between the parties. Since the minimal amount of communication that the parties can exchange in any such run is one bit, it follows that at least one bit of communication is necessary to simulate

these correlations. For qubits, i.e, when $d = 2$, one bit is known to be sufficient [20]. For other values of d , it is possible to extend our analysis by letting the range of measuring settings go from 1 to $(d-1)N$, while keeping the measurements as defined in (5) and (6). Using inequalities similar to (3), one can then show that at least $\log_2 d$ bits of communication are necessary. This bound is not optimal asymptotically since for large d a bound of $O(d)$ bits is known [21]. It may, however, be useful for small d .

Summary and conclusions. The quantum correlations introduced imply that maximally entangled quantum states in arbitrary dimensions have zero local component. They motivate experiments that could bound the weight of the local component as close to zero as possible. In a non-signalling context, the correlations are also provably monogamous, which gives them an immediate application in key distribution. It would be interesting to characterise the sets of quantum correlations that are monogamous in this sense; in particular, it would be interesting to know if there are monogamous quantum correlations that can be obtained in an experiment with only a finite number of measurement settings at each site, rather than in the limit in which the number of settings tends to infinity.

Acknowledgments. AK thanks Jonathan Oppenheim for helpful conversations. SP acknowledges support by the David and Alice Van Buuren fellowship of the Belgian American Educational Foundation, by the National Science Foundation under Grant No. EIA-0086038, and by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848.

* jbarrett@perimeterinstitute.ca

† a.p.a.kent@damtp.cam.ac.uk

‡ Stefano.Pironio@icfo.es

- [1] J. S. Bell, *Speakable and unspeakable in quantum mechanics* (Cambridge University Press, Cambridge, 1987).
- [2] W. Tittel and G. Weihs, *Quant. Inf. Comp.* **1**, 3 (2001).
- [3] G. Brassard, *Found. Phys.* **33**, 1593 (2003).
- [4] J. Barrett, L. Hardy, and A. Kent, *Phys. Rev. Lett.* **95**, 010503 (2005).
- [5] A. Elitzur, S. Popescu, and D. Rohrlich, *Phys. Lett. A* **162**, 25 (1992).
- [6] The assumption made in Ref. [5] is that the correlation function $E_L(\theta)$ introduced in the paper has an expansion in θ for small, positive θ .
- [7] R. F. Werner and M. M. Wolf, *Quant. Inf. Comp.* **1**, 1 (2001).
- [8] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic Publishers, Dordrecht, 1989), p. 69.
- [9] N. D. Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990).
- [10] P. Heywood and M. Redhead, *Found. Phys.* **13**, 481

- (1983).
- [11] A. Cabello, Phys. Rev. Lett. **87**, 010403 (2001).
 - [12] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002). The notation is taken from A. Acín, R. D. Gill, and N. Gisin, Phys. Rev. Lett. **95**, 210402 (2005).
 - [13] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
 - [14] P. A. Pearle, Phys. Rev. D **2**, 1418 (1970).
 - [15] S. L. Braunstein and C. M. Caves, Ann. Phys. **202**, 22 (1990).
 - [16] L. Hardy, Phys. Lett. A **161**, 21 (1991).
 - [17] J. Barrett, L. Hardy, and A. Kent, unpublished; A. Kent, Perimeter Institute seminar on April 2, 2003, archived at www.perimeterinstitute.ca.
 - [18] A. Acín, N. Gisin, and L. Masanes, quant-ph/0510094.
 - [19] S. Pironio, Phys. Rev. A **68**, 062102 (2003).
 - [20] B. F. Toner and D. Bacon, Phys. Rev. Lett. **91**, 187904 (2003).
 - [21] G. Brassard, R. Cleve, and A. Tapp, Phys. Rev. Lett. **83**, 1874 (1999).